Cyber Securing CSOs in the Digital Age

Safe digital space

Based on the workshop organized by VANI
(Notes compiled by V.Selvakumar)
UTTHAN *36, Chitrakut Twins, B/h Management Enclave, Nehru Park, Vastrapur, Ahmedabad Gujarat 380015*

BACKGROUND

On April 15th, the webinar "Cyber Securing CSOs in the Digital Age," organized by VANI in association with Digital Empowerment Foundation, provided nonprofit leaders and civil society organizations (CSOs) with a vital platform to address the escalating significance of cybersecurity in today's digital landscape. With technology playing an increasingly integral role in CSO operations and outreach, safeguarding sensitive data, defending against cyber threats, and ensuring digital resilience have become imperative. This event aimed to equip CSOs with the requisite knowledge, tools, and strategies to effectively navigate the complex cybersecurity landscape. Discussions covered understanding the latest cyber threats, implementing robust security measures, and fostering a culture of cyber awareness. The insights shared aimed to empower CSOs to fortify their cybersecurity posture and protect their mission-critical assets in the digital age.

COMMON CYBERTHREATS

1. Phishing or Spear Phishing:
    - Definition: Deceptive attempts to acquire sensitive information by posing as a trustworthy entity via emails or messages.
    - Example: A fraudulent email claiming to be from a bank, asking recipients to update their account details by clicking on a malicious link.
2. Vishing (Voice Phishing):
    - Definition: Scams conducted over the phone, where attackers manipulate individuals into providing personal information.
    - Example: A caller pretending to be a bank representative, asking for account details to "verify" the account.
3. Business Email Compromise (BEC):
    - Definition: Sophisticated email scams targeting businesses, often involving impersonation of company executives to trick employees into transferring funds or sensitive information.
    - Example: An email impersonating the CEO instructing the finance department to wire money to a fraudulent account.
4. Baiting:
    - Definition: Luring victims into a trap by offering something enticing, like a free download or USB drive, which contains malware.
    - Example: Leaving infected USB drives labeled as "Company Payroll" in a parking lot, hoping an employee will pick one up and plug it into their work computer.
5. Password Attacks:
    - Definition: Attempts to gain unauthorized access to user accounts by exploiting weak or stolen passwords.
    - Example: Using automated tools to guess passwords or trying commonly used passwords to gain access to an online account.
6. Watering Hole Attacks:
    - Definition: Infecting websites frequented by target victims with malware, exploiting their trust in those sites.

- Example: Compromising a popular industry forum website frequented by employees of a targeted company with malware.

7. Pretexting:
    - Definition: Creating a false pretext or scenario to trick individuals into disclosing sensitive information or performing actions.
    - Example: Posing as a bank employee and calling a customer, claiming there has been suspicious activity on their account and requesting their login details to "verify" their identity.
8. Malware and Spyware:
    - Definition: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or secretly gather information.
    - Example: A malware-infected attachment in an email that, when opened, installs a virus on the victim's computer.

9. Credential Surfing:
    - Definition: Using stolen login credentials from one website or service to gain access to other accounts belonging to the same individual.
    - Example: Using the same username and password obtained from a compromised social media account to log in to the victim's email account.
10. Keylogging:
    - Definition: Recording keystrokes on a computer or mobile device to capture sensitive information.
    - Example: Installing software on a victim's computer that records every keystroke, allowing attackers to capture usernames, passwords, and other sensitive information.
11. Ransomware:
    - Definition: Malware that encrypts files or locks systems, demanding payment for decryption or to unlock the system.
    - Example: A ransomware virus encrypting all files on a victim's computer and demanding payment in Bitcoin for the decryption key.
12. Honey Trap:
    - Definition: Manipulating individuals into revealing information or performing actions by exploiting their emotions or desires.
    - Example: A spy seducing a target to extract sensitive information or gain access to secure areas.
13. Quizzing:
    - Definition: Posing as legitimate entities and asking security questions to gather sensitive information.
    - Example: A scammer posing as a technical support representative calling a victim and asking for personal information, claiming it's needed to fix a computer issue.
14. Man-in-the-Middle (MitM) Attacks:
    - Definition: Intercepting communication between two parties to eavesdrop, modify, or impersonate messages.
    - Example: A hacker intercepting communication between a user and their bank's website, capturing login credentials and personal information.

15. Distribution Denial of Service (DDoS) Attacks:
    - Definition: Overwhelming a target server or network with traffic, rendering it inaccessible to legitimate users.
    - Example: Flooding a website's server with a massive amount of traffic, causing it to crash and become unavailable to users.
16. Supply Chain Attacks:
    - Definition: Targeting the weakest link in a supply chain to compromise larger organizations.
    - Example: Cybercriminals compromising a software vendor's update mechanism to distribute malware to the vendor's customers.

SAFETY MEASURES TO PROTECT FROM CYBERTHREATS

1. Use secure, encrypted connections:
    - Install browser extensions like HTTPS Everywhere to automatically ensure secure connections whenever possible.
    - Verify that websites display a padlock icon in the address bar, indicating a secure connection.
2. Avoid Public Wi-Fi:
    - Use your smartphone's cellular data connection or a personal hotspot instead of public Wi-Fi when accessing sensitive information.
    - Consider investing in a portable Wi-Fi hotspot device for secure internet access on the go.
3. Use Strong Unique Passwords:
    - Use a passphrase consisting of multiple words, numbers, and symbols to create a strong, memorable password.
    - Consider using a password manager like LastPass, Dashlane, or Bitwarden to securely store and manage your passwords.
4. Enable Multi-Factor Authentication (MFA):
    - Use authenticator apps like Google Authenticator or Authy instead of SMS-based verification for MFA, as they provide stronger security.
    - Keep backup codes for MFA in a secure location in case you lose access to your primary authentication method.
5. Backup Important Data:
    - Set up automatic backups on a regular schedule to ensure that your data is consistently protected.
    - Test your backup systems periodically to ensure they are working properly and that you can restore your data if needed.
6. Be Cautious with Links and Email Attachments:
    - Hover over links in emails to preview the URL before clicking on them, especially if the email seems suspicious.
    - Use online tools like VirusTotal to scan email attachments or suspicious files before opening them.
7. Avoid Downloading from Untrusted Sources:

- Check app reviews, ratings, and developer information before downloading apps from app stores to ensure their legitimacy.
- Consider using built-in app stores like Google Play Store or Apple App Store, which have stricter security measures in place.

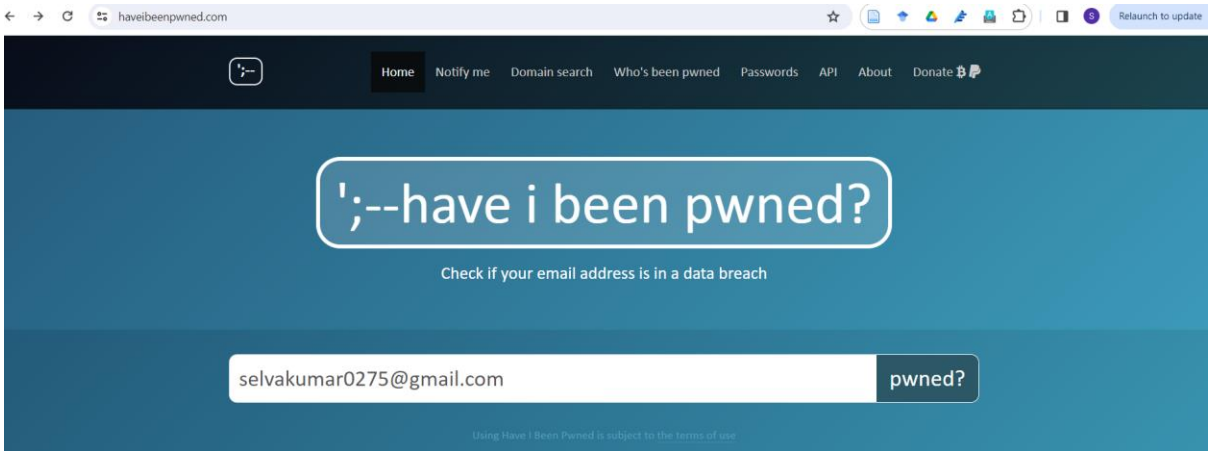
8. Regularly Scan Your Device:
    - Schedule automatic scans during off-peak hours to minimize disruptions while ensuring your device remains protected.
    - Configure your antivirus software to update definitions automatically to detect the latest threats.
9. Use Email Filters:
    - Customize your email filters to flag or automatically delete suspicious emails based on keywords, sender addresses, or other criteria.
    - Train your email filter by marking spam emails as junk to improve its accuracy over time.
10. Update Your Devices:
    - Enable automatic updates for your operating system, software, and apps to ensure timely installation of security patches.
    - Set reminders to manually update devices that do not support automatic updates, such as smart home devices or older hardware.
11. Enable Privacy Settings:
    - Regularly review and update privacy settings on social media platforms to restrict who can see your personal information and posts.
    - Limit the permissions granted to apps and services to access your personal data, and revoke permissions for apps you no longer use.

12. Google fishing identification Quiz:
    - The website "https://phishingquiz.withgoogle.com/" is an educational resource provided by Google to help users learn how to identify phishing emails and protect themselves from cyber threats. The quiz presents users with a series of interactive scenarios simulating common phishing tactics and asks them to determine whether each scenario is a legitimate email or a phishing attempt. Through this engaging and informative quiz, users can enhance their awareness of phishing techniques and improve their ability to recognize and avoid potential risks online.

DATA BREACH IDENTIFICATION

"Have I Been Pwned" (HIBP) is a website created by security researcher Troy Hunt that allows users to check if their personal information has been compromised in data breaches. Here's a brief overview:

1. **Data Breach Monitoring**: HIBP collects and aggregates data from various publicly disclosed data breaches. It allows users to search for their email addresses or usernames to see if they have been involved in any known data breaches.



COMMUNICATION AND DATA SHARING BEST PRACTICES

1. **Use secure, end-to-end encrypted Messaging Channels:**
    - Example: Utilize messaging apps like Signal or WhatsApp, which offer end-to-end encryption, ensuring that only the sender and recipient can read the messages.
2. **Turn on the Disappearing Chat option:**
    - Example: Enable disappearing messages in messaging apps like Telegram or Snapchat to automatically delete messages after a set period, reducing the risk of sensitive information being stored indefinitely.
3. **Use a Secured platform for File Sharing:**
    - Example: Utilize secure file-sharing platforms like Dropbox or Google Drive, which provide encryption and access controls to ensure that only authorized users can view or edit shared files.
4. **Ensure proper settings are in place for secure communications apps:**
    - Example: Configure security settings in apps like Microsoft Teams or Slack to enable features such as end-to-end encryption, multi-factor authentication (MFA), and access controls for users and channels.
5. **Use Cloud-based Email Services:**
    - Example: Employ cloud-based email services like Gmail or Microsoft 365, which offer robust security features such as spam filtering, encryption, and advanced threat protection.
6. **Frequently remind the organization about security best practices related to group messaging and metadata:**
    - Example: Conduct regular security awareness training sessions for employees, emphasizing the importance of avoiding sensitive information in group chats and understanding the risks associated with metadata exposure.
7. **Store sensitive data exclusively in a trusted cloud storage service:**

- Example: Store confidential documents and files in a secure cloud storage service like Amazon S3 or Microsoft OneDrive, which provide encryption at rest and in transit to protect data from unauthorized access.

8. **Enable 2FA to Cloud Storage:**
    - Example: Implement two-factor authentication (2FA) on cloud storage accounts such as Dropbox or Box to add an extra layer of security and prevent unauthorized access to sensitive data.
9. **Set and enforce a policy to limit sharing settings within the cloud:**
    - Example: Establish guidelines specifying who can share files externally and restrict sharing settings to prevent accidental exposure of sensitive information.
10. **If your organization opts to store data locally, invest in skilled IT staff:**
    - Example: Hire experienced IT professionals to manage local servers and databases, ensuring proper security measures are implemented to protect sensitive data from unauthorized access or breaches.
11. **Keep data backups secure - encrypt backup hard drives or other backup devices:**
    - Example: Encrypt external hard drives or USB drives used for data backups using tools like BitLocker (for Windows) or FileVault (for macOS) to prevent unauthorized access to backup data in case of theft or loss.

SOCIAL MEDIA SAFETY

1. **Develop an Organizational Social Media Policy:**
    - Example: Create guidelines outlining acceptable behavior, confidentiality measures, and security protocols for employees when using social media platforms on behalf of the organization.
2. **Develop an anti-harassment infrastructure within your organization:**
    - Example: Implement reporting mechanisms and support systems to address instances of harassment or abuse on social media platforms involving employees or associated individuals.
3. **Enable Privacy Settings:**
    - Example: Adjust privacy settings on social media accounts to control who can view posts, photos, and personal information, limiting exposure to unauthorized users.
4. **Review Your Friend list:**
    - Example: Regularly review and remove individuals from your social media friend list whom you no longer interact with or whose identities you cannot verify.

5. **Delete Unused Accounts:**
    - Example: Close or deactivate social media accounts that are no longer actively used to minimize the risk of unauthorized access or account compromise.
6. **Limit Photo Tagging and Control Who Can Tag You:**
    - Example: Adjust settings to approve tags before they appear on your profile and limit who can tag you in photos to prevent unauthorized tagging or privacy violations.
7. **Diversify Usernames:**
    - Example: Use unique usernames across different social media platforms to minimize the risk of account takeover or impersonation.
8. **Monitor Access to Third-Party Apps:**
    - Example: Regularly review and revoke access permissions granted to third-party apps or services connected to your social media accounts to prevent data misuse or unauthorized access.
9. **Addressing Security Alerts:**
    - Example: Take immediate action in response to security alerts from social media platforms, such as suspicious login attempts or unrecognized devices accessing your account.
10. **Enable DDoS Protection for Your Website, like Google's Project Shield:**
    - Example: Implement Distributed Denial of Service (DDoS) protection services such as Google's Project Shield to mitigate the impact of DDoS attacks and ensure uninterrupted access to your organization's website.
11. **Host Your Organization's Website Securely:**
    - Example: Utilize secure web hosting services with SSL/TLS encryption, regular security updates, and robust access controls to protect sensitive data and prevent unauthorized access.
12. **Protect Your Wi-Fi Networks by Using Strong Passwords:**
    - Example: Secure Wi-Fi networks with strong, unique passwords, and enable encryption (such as WPA2 or WPA3) to prevent unauthorized access and data interception by malicious actors.

10 COMMANDMENTS FOR CYBERSECURITY

1. **Organize periodic security awareness sessions for your team:**
    - Example: Conduct regular training sessions for employees to educate them about cybersecurity best practices, such as recognizing phishing emails, creating strong passwords, and identifying security threats.
2. **Stay vigilant against phishing attempts and establish a reporting mechanism:**

- Example: Implement a process for employees to report suspicious emails or phishing attempts to the IT department, enabling prompt action to mitigate potential risks and prevent security breaches.

3. **Prioritize encryption for all communication, especially end-to-end:**
    - Example: Use encrypted messaging apps like Signal or WhatsApp for sensitive communications to ensure that messages and data are secure from interception by unauthorized parties.
4. **Keep all employee devices and software current with regular updates:**
    - Example: Enforce policies requiring employees to regularly update their devices, operating systems, and software applications to patch known vulnerabilities and protect against cyber threats.
5. **Safeguard data with secure cloud storage solutions:**
    - Example: Utilize cloud storage services like Dropbox Business or Microsoft OneDrive for Business, which offer encryption, access controls, and data backup features to protect sensitive information from unauthorized access or loss.
6. **Utilize HTTPS and, if necessary, employ a VPN for internet access:**
    - Example: Ensure that employees use secure HTTPS connections when browsing websites and consider implementing a virtual private network (VPN) for remote work to encrypt internet traffic and protect data from interception.
7. **Enforce the use of robust passwords and deploy a company-wide password manager:**
    - Example: Implement password policies requiring employees to create strong, unique passwords and use a password manager like LastPass or Dashlane to securely store and manage credentials.
8. **Secure physical assets to prevent unauthorized access:**
    - Example: Implement physical security measures such as access control systems, surveillance cameras, and secure locks to safeguard company premises, equipment, and sensitive information stored on physical media.
9. **Create a comprehensive incident response plan for your organization:**
    - Example: Develop and document an incident response plan outlining procedures for detecting, responding to, and recovering from cybersecurity incidents such as data breaches, malware infections, or system compromises.
10. **Implement two-factor authentication wherever feasible:**
    - Example: Enable two-factor authentication (2FA) on all critical systems, applications, and online accounts to add an extra layer of security beyond passwords and protect against unauthorized access.